UDC 004.056.53

Security of fingerprints in biometric authentication systems using cryptography and watermarking technique

Zaripov N.N.
Teacher of Department of Information Technology, Bukhara State University

Foydalanuvchi autentifikatsiya tizimlarida barmoq izi yordamida tanish ishonchli yechim hisoblanadi. Ushbu maqolada kriptografiya va moybo'yoqli yondashuv yordamida barmoq templeydi himoyasiga asoslangan xavfsiz autentifikatsiya modeli keltirilgan.
Tayanch iboralar: *barmoq templeydi, biometrik autentifikatsiya, moybo'yoqli barmoq izi, shifrlash.*

Безопасность отпечатков пальцев в биометрических системах аутентификации с использованием криптографии и технику водяных знаков

Распознавание отпечатков пальцев является надежным решением в системах аутентификации пользователей. Эта статья посвящена определению защищенной модели аутентификации, основанной на защите шаблонов отпечатков пальцев, используя подходы, криптографии и водяных знаков.
Ключевые слова: *темплейд отпечатка пальца, биометрическая аутентификации, отпечатка пальца водяным знаком, шифрование.*

Kriptografiya va moybo`yoqli texnika yordamida biometrik autentifikatsiya tizimlarida barmoq izlari xavfsizligini taminlash

Fingerprint recognition is a reliable solution in user authentication systems. This paper deals with the definition of a secure authentication model, based on fingerprint template protection by using the approaches of cryptography and watermarking.
Keywords: *fingerprint template, biometric authentication, watermarked fingerprint, encryption.*

Introduction

Identity recognition is still an open problem and its solution can help for user authentication, the secure access to restricted areas and, more generally, anytime it is necessary to automatically acquire the identity of a human operator. It is worth to point out that the application of an identity recognition system can go beyond security issues, being the basic for a more sophisticated human machine interface in a pervasive context. A person can be identified through the analysis of her physical peculiar features: automated methods and algorithms for feature acquisition, analysis and recognition stand at the core of biometrics.

A biometric identifier is a physiological or behavioral characteristic of a person such as face features, iris, palm, fingerprint, hand or finger geometry, retina, voice, handwritten signature, keystroke dynamics, etc., that are strictly linked to each person and cannot be easily tampered with. Basically, all them are unique, universal, unalterable, and can be measured. Due these properties, biometrics have been used to identify or authenticate users in a biometric system, which is becoming more popular than traditional

identification techniques such as identification card (ID), password and personal identification number (PIN). In the recognition process acquired raw data are preprocessed to extract relevant geometric arrangements of features that are then compared and matched to those that form the user template stored in a backend database.

Biometric systems are based on the following steps [5]: first, a biometric sample is taken from an individual, for example iris scan; then, this biometric can be presented as an image or some data are extracted from that sample which constitute a biometric template; finally, the biometric data, either the image or the template or both, are stored on a database or in a smart card. All these steps constitute the process known as enrollment. One time a person performs the enrollment process, he/she can identify (distinguish an individual from a larger set of individual biometric records, i.e. one-to-many matching) or authenticate (a live biometric sample presented by a person is compared with a stored sample, i.e. one-to-one matching) by presenting his/her biometric sample in the system, which will compare the submitted sample with stored sample and if the matching process succeeds, the person is recognized and the system will accept him/her. In other case, she/he is not recognized, i.e. will be rejected. Talking about the reliability of a biometric system, the submitted sample (actual) can present some variance with the stored reference sample, which could make of the comparison, matching and identification, an inexact process, i.e. the biometric system does not have 100% of accuracy. There are two metrics to measure the accuracy of a biometric system, false rejection rate (FRR) and false acceptance rate (FAR). FRR is how many rejects (incorrectly) performs the bio- metric system, i.e. when the system rejects a legitimate user. FAR is how many acceptances (incorrectly) performs the biometric system, i.e. when the system incorrectly match a biometric sample with a wrong stored reference sample, resulting in misidentification. The ranges of FRR for most biometric system are from 0.1% to 20%, i.e. a legitimate user will be rejected one of 1000 times and one to 5 times on average [2].

Nevertheless, the biometric systems present some security concerns related with secrecy of personal data and identity theft. Basically there are four types of attack in a generic biometric system: attack on sensor, attack between modules, software attack and attack against the biometric template stored in database. The last kind of attack is the most dangerous in a biometric system because the biometric template can be replaced by an impostor to compromise the security of the system. In addition, the user will lost its biometric trait for ever (identity theft) and he/she cannot use it further for authentication due it is irrevocable, i.e. the authorized user can not generate two different fingerprint traits from the same finger. Therefore, biometric template protection is required a biometric systems to increase the security in both the biometric system and personal biometric protection [1].

Due to these security challenges, there are an increasing interest to design, built and implement secure biometric template protection in biometric systems.

There are four major requirements when a biometric template protection algorithm is designed [3]:

- ♣ Revocability. Ability of the algorithm to cancel the compromised template and generate a new one from the same biometric trait.
- ♣ Diversity. The secure biometric template must not allow cross-matching across databases, thereby ensuring the users privacy.

♣ Security. Extract the original template from the protected template must be computationally difficult to achieve. This ensures the secrecy of the user's biometric template.

♣ Performance. The protecting algorithm should not affect the recognition performance of the biometric system, i.e. the FAR and FRR rates need to be acceptable.

Cryptography and watermarking are other approaches to protect sensitive information against not authorized users. Watermarking is used for the copyright protection. Cryptography is a technique thoroughly used on secure communications and private data storing, where the plain data are transformed in encrypted data by using an algorithm and secret key. Although, these schemes do not guarantee revocation and they are not recommend for biometric protection because the matching process requires decryption of stored templates and the security depends of the cryptographic key the cryptographic method can achieve a very high security and it can be verified with several security analysis at statistical level (where several approaches fail).

Watermarking is used for hiding information imperceptibly in digital content for protecting its integrity. A number of watermarking techniques are available for embedding information securely in an image. Recently watermarking techniques have been used in conjunction with biometric identifiers. Fingerprints are one of the reliable biometric identifiers that are extensively used for personal identification.

In this paper, we proposed a novel embedded fingerprint authentication system by using an encryption algorithm and watermarking technique. The proposed biometric scheme protections are based on features transform, but the matching process is performing in plain domain and decryption template is required. The implementation is based in an embedded expert system with high accuracy, secure enrollment and authentication process, with fingerprint template protection. The security of the proposed scheme is verified with a complete statistical security analysis and a hardware analysis such as architecture, memory space, communication ports, frequency system, speed, precision and others.

Main part

Extraction of fingerprint texture features. Texture is an important feature for the analysis of many types of images. Properties such as roughness, granulation and regularity which do not have smooth varying intensities can be determined through a set of local neighborhood properties of the gray levels of an image region. Multi-scale processing which, humans apply for texture perception is modeled using wavelet analysis [4]. The image features that represent the scale-dependent properties can be extracted from each sub-image separately. A non-linear function that produces the energy of the image when summed over a sub-image is widely used for texture computation. The feature set thus obtained consists of energies of different scales, which is an important characteristic for texture analysis. A signal $f(x)$ when decomposed using a one-dimensional wavelet transform into a basis of wavelet functions to obtain the transformed signal, $W_{p,q}$ is given by

$$W_{p,q}(f(x)) = \int f(x) \cdot \psi_{p,q}(x) dx \quad (1)$$

where, p and q are scale and position parameters, respectively. The basis vectors are

obtained by translating and dilating the mother wavelet:

$$\psi_{p,q}(x) = \frac{1}{p} \cdot \psi\left[\frac{x-q}{p}\right] \tag{2}$$

The mother wavelet ψ has to be localized in both spatial and frequency domains. A two-dimensional wavelet transform is obtained by first applying a one-dimensional transform along the rows and then along the columns. In this paper, a Daubechies filter bank is used to implement the discrete wavelet transform (DWT) resulting in a pyramid structure of sub-bands shown in Fig. 1. The two-level decomposition consists of seven sub-bands. The sub-bands labeled HH, HL and LH contain the diagonal, horizontal and vertical details of the fingerprint image, respectively, while the LL sub-band contains the coarse details of the image.

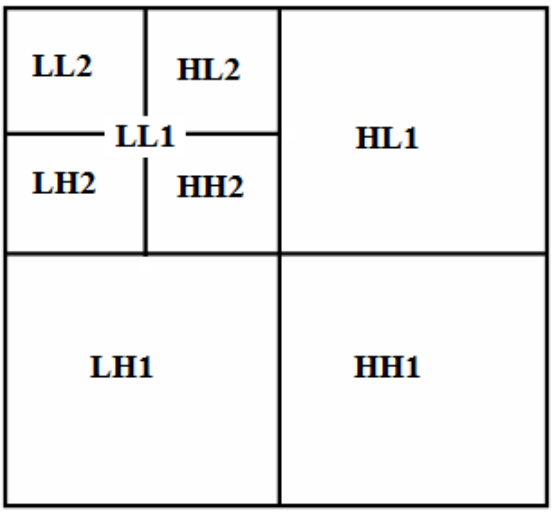


Figure 1. Two level decomposition using DWT

In this paper, the face and the demographic text data are used as contextual watermarks and are embedded in the fingerprint image to be authenticated. The grayscale fingerprint image is decomposed using two-level discrete wavelet transform to obtain seven sub-bands as shown in Fig. 1. The text and face watermark images are embedded into the wavelet coefficients of the fingerprint image that represent the locations of the selected texture regions. The facial image is in grayscale while the text image is in binary. The sub-image selection for watermarking depends on several factors. The modification of the low frequency sub image LL2 will impose severe degradation of the reconstructed image as most of the energy is concentrated in this band. During filtering and compression some of the information will be lost in the high frequency bands. One way of overcoming this information loss is by redundantly embedding information in all the high frequency bands (LH1, HL1 and HH1). The mid-frequency bands (LH2, HL2 and HH2) are good choices for embedding. We embed the grayscale face image into the mid-frequency bands and the binary text image is redundantly embedded into the high frequency bands for increased robustness. The final watermarked fingerprint image is obtained when the embedded sub-b ands are reconstructed using a two-level inverse discrete wavelet transform (IDWT).

Image watermarking. The digital watermarking system essentially consists of a

watermark embedder and a watermark detector (Figure 2). The watermark embedder inserts a watermark onto the cover signal and the watermark detector detects the presence of watermark signal. Note that an entity called watermark key is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark signal (i.e., a unique watermark key exists for every watermark signal). The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks (Fig. 2.).

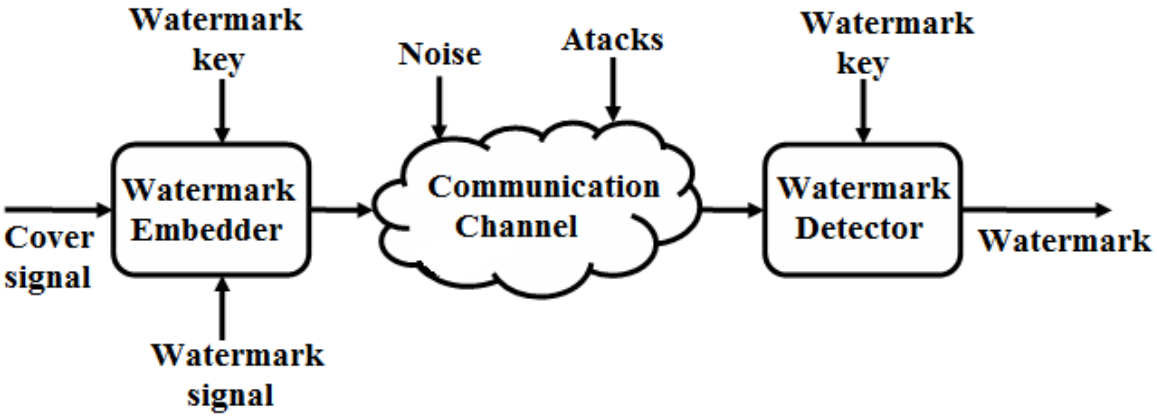


Figure 2. General watermarking system

Watermarking techniques should be tamper resistant to hostile attacks. Depending on the application, the watermarked content encounters certain types of attacks. Some types of attacks are more important than others. Some basic types of attack are [6]:

- ♣ Active attacks
- ♣ Passive attacks
- ♣ Collusion attacks
- ♣ Forgery attacks

Proposed authentication process scheme. A watermark, which is often consists of a binary data sequence, is inserted into a host signal with the use of a key. The information embedding routine imposes small signal changes, determined by the key and the watermark, to generate the watermarked signal. This embedding procedure involves imperceptibly modifying a hoist signal to reflect the information content in the watermark so that the changes can be later observed with the use of the key to ascertain the embedded bit sequence. The process is called watermark extraction.

Watermark Embedding

Input:

Cover Image – gray scale fingerprint image, to be watermarked.

Face image – a binary image act as a watermark .

Demographic data image– a binary image act as watermark.

E1 – key used to encrypting IDWT.

E2 – key used for encrypting face image and demographic data image watermarks.

W – key used to watermarked embedder, encrypted watermark in Cover Image.

Output:

Watermarked fingerprint – finally watermarked image.

Fig. 3 shows the proposed watermarking algorithm used for embedding the face and the text images in the fingerprint.

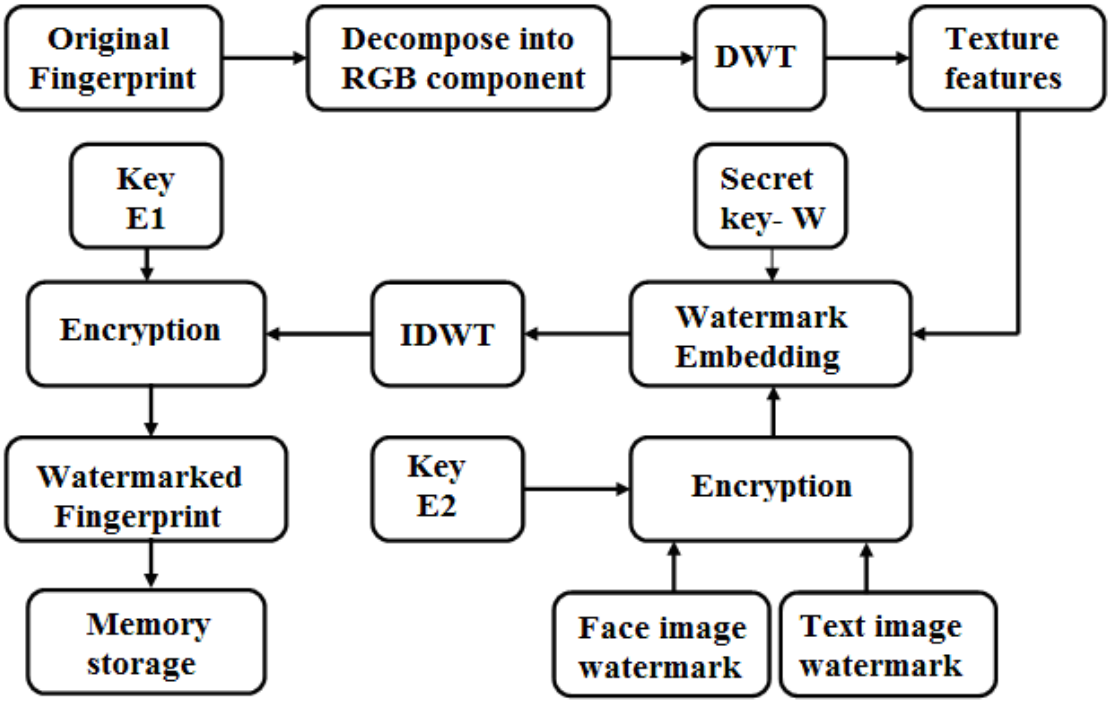
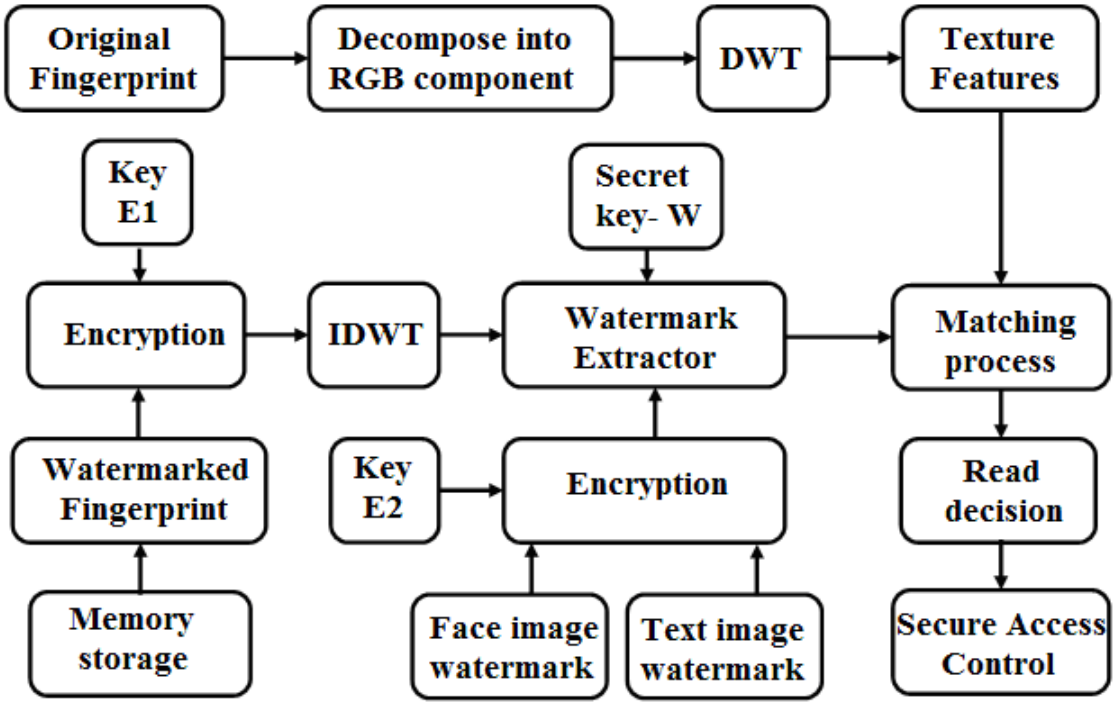


Figure 3. Enrollment process scheme

The resulting watermarked fingerprint is securely protected and can be used to verify if the chain of custody is maintained or if the fingerprint has been compromised by tampering. Using the same technique, the facial image is extracted from the lower frequency channel. Neither the original fingerprint image nor the original watermark images are required for extraction. The contextual watermarking approach using face and text images and encryption to watermark a fingerprint is useful for authenticating the integrity of the fingerprint. The watermarked fingerprint image is compact and takes less memory space compared to the space occupied by individual images. Furthermore, the time taken to search different database to obtain all pertinent information corresponding to an individual is greatly minimized since each fingerprint image has the demographic text and face image embedded as watermarks and can be easily extracted.

Finally, the authentication process is achieved on fingerprint module with its matching algorithm. If the templates are the same, the user has access to the restricted area (Fig. 4).

The watermarked fingerprint was shown to be robust and resilient when subjected to various attacks. Unauthorized tampering or substitution of the fingerprint data can be detected by extracting the watermarks. Since the visual quality of the text and the face images are commonly used for personal identification, it is appropriate to use the human visual metrics for comparison purposes.



Figur 4. Authentication process scheme

Conclusion

In this work, we proposed a secure authentication with fingerprint template based on watermarking and cryptography. In addition two watermarks, a facial image and the corresponding demographic text data of an individual are secure embedded into selected texture regions of fingerprint image using discrete wavelet transform. The watermarked fingerprint provides added protection from tampering and the fingerprint matching ability is not affected even when subjected to common attacks. For extracting the embedded face and text images, the original images are not required. One of the main advantages is that the fingerprint, the demographic text information of the individual and the facial image need not be stored in separate databases. Using the proposed approach, the absence of watermarks or visual distortions in the extracted watermarks would reveal that the integrity of the fingerprint image has been compromised. The proposed scheme has high potential in several applications in both simple embedded system or embedded expert systems such as control access in offices, banks, factories, hospitals, universities, e-commerce and others.

REFERENCES

1. Admek, M., Matsek, M., & Neumann, P. Security of biometric systems. 25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM, 2014, pp. 169 – 176.

2. Cavoukian, A., Stoianov, A. Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy. Information and Privacy Commissioner of Ontario 48, 2007.

3. Jain, A. K., Nandakumar, K., & Nagar, A. Fingerprint template protection: From theory to practice. In Security and privacy in biometrics. London: Springer, 2012, pp. 187 – 214.

4. M. Kociolek, A. Materka, M. Strzelecki, P. Szczypinski, Discrete wavelet transform-derived features for digital image texture analysis, in: Proceedings of the International Conference on Signals and Electronic Systems, 2001, pp. 163 – 168.

5. M.A. Murillo-Escobar, C. Cruz-Hernandez, F. Abundiz-Perez, R.M. Lopez-Gutierrez. A robust embedded biometric authentication system based on fingerprint and chaotic encryption. Expert System with Applications 42, 2015, pp. 8198 – 8211.

6. William Stallings, "Cryptography And Network Security Principles And Practice", 5th ed., NY, Pearson Education, Inc., 2011, pp. 809 – 812.